Security and Administration

The Cisco Smart PHY application is hosted on a Cisco Operations Hub cluster. Cisco Operations Hub provides the following authentication services for Cisco Smart PHY:

- Basic authentication
- LDAP authentication

Switching the authentication method of Cisco Smart PHY from the default Basic authentication to LDAP authentication, and vice versa, is accomplished through the Cisco Operations Hub Operation Center CLI. The procedures for switching between the authentication methods are provided in this section.

Switch from Basic Authentication to LDAP Authentication

The Operations Hub `ops-center` CLI allows an administrator to configure LDAP settings for external authentication with AD (Active Directory).

Note LDAP support is limited to Microsoft Active Directly (AD) only. Open LDAP is not supported.

Procedure

Step 1 Access the Operations Hub ops-center by using the following URL:

```
https://cli.opshub-data-ops-center.{FQDN}/
```

```
https://cli.opshub-data-ops-center.<Cisco Smart PHY master virtual IP address>.nip.io}/
```

Step 2 Log in to the Operations Hub ops-center CLI.

The administrator can log into the Operations Hub ops-center CLI using the `admin` username and its password that is created while deploying the Operations Hub.

Example:

```
product opshub# config t
Entering configuration mode terminal
product opshub(config)# ldap-security ldap-server-url ******
product opshub(config)# ldap-security ldap-username-domain ******.com
product opshub(config)# ldap-security base-dn DC=******,DC=com
product opshub(config)# ldap-security ldap-filter userPrincipalName=%s@******.com
product opshub(config)# ldap-security group-attr memberOf
product opshub(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Step 3 Configure the mapping between the LDAP groups and the API groups.

Example:

```
product opshub(config)# ldap-security group-mapping ?
Possible completions:
  LDAP group
product opshub(config)# ldap-security group-mapping {ldap group}} ?
Possible completions:
  <NACM group>  admin  api-admin  api-editor  api-viewer
product opshub(config)# ldap-security group-mapping {ldap group}} api-admin
product opshub(config-group-mapping-crdc-docsis/api-admin)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Switch from LDAP Authentication to Basic Authentication

Procedure

Step 1 Log in to any one of the control-plane nodes using the following command:

```
ssh -i <private-key-file> <smartphy-user>@<control-plane-node-ip>
```

Step 2 Enter the following command.

```
kubectl get svc ops-center-smartphy-data-ops-center -n smartphy-data
```

Note the cluster IP address and TCP ports of the service ops-center-smartphy-data-ops-center.

```
Ops-center-smartphy-data-ops-center    ClusterIP     10.x.x.x    <none>
    8008/TCP,8080/TCP,2024/TCP,2022/TCP,7681/TCP        19d
```

Step 3 Enter the following command to log in to the service resource using the password previously set by the auto-deployer.

```
ssh admin@<cluster-ip-of-svc> -p <port-number>
```

Example:

```
smartphyuser: ~$ ssh admin@10.x.x.x -p 2024
Warning: Permanently added '[10.x.x.x]:2024' (RSA) to the list of known hosts.
admin@10.x.x.x's password:
Welcome to the smartphy CLI on user/data
admin connected from172.x.x.x using ssh on
ops-center-smartphy-data-ops-center-774b8cc6fb-n6qmz
[user/data] smartphy#
```

Step 4 Run the following command to enter the configuration mode and get a list of available commands.

```
config
```

Use the `kong` command and its sub-commands.

Step 5 Enable the Basic authentication plugin regardless of the status of LDAP authentication plugin.

```
kong ldap_plugin enable false
```

Step 6 Enter the `commit` command to save the changes and start using the Basic authentication plugin.

Step 7 Enter `end` to exit the config mode and enter `exit` to exit the service resource.

Basic authentication plugin is enabled and you can log in to the UI using a local existing username and password.

Renew Kubernetes Client TLS Certificate

Cisco Smart PHY leverages Kubernetes for container orchestration. During the Cisco Smart PHY cluster deployment, Kubernetes client TLS certificates are created to secure the communication between the Kubernetes API server and kubelets. Kubernetes client TLS certificates are valid for one year.

Caution Renew the Kubernetes client TLS certificates before they expire. Otherwise, the operation and functionality of the Cisco Smart PHY cluster will be impacted.

Administrators can check the current status of the Kubernetes certificates by running the following command in the Linux shell:

```
sudo openssl x509 -enddate -noout -in /data/kubernetes/pki/kubelet-client-current.pem
```

The certificates are valid through the date that is listed in the attribute `notAfter=`.

For more information on renewing the Kubernetes Client TLS Certificate, contact your Cisco Account Team.

Add Users using Cisco Operations Hub CLI

The Cisco Operations Hub ops-center CLI allows the administrator to create new users.

The Cisco Operations Hub ops-center URL is `https://cli.opshub-data-ops-center.{hostname}/`. The administrator can log into the Cisco Operations Hub ops-center CLI using the `admin` username and its password that is created while installing Cisco Smart PHY application.

```
product opshub# smiuser show-user username admin
User: admin, Group(s): admin api-admin api-editor api-viewer li-admin, Password Expiration
 days: 86
```

Add Users

Use the following procedure to create a new user:

Procedure

Step 1 Define a new user using the following sample commands:

```
product opshub# smiuser add-user username <username> password <password>
message User added
product opshub#
product opshub# smiuser show-user username <username>
User: <username>, Group(s): <username>, Password Expiration days: -1
```

Example:

```
product opshub# smiuser add-user username user123 password Abcd123@
message User added
product opshub#
product opshub# smiuser show-user username user123
User: user123, Group(s): user123, Password Expiration days: -1
```

Step 2 Add a new user to the API group using the following commands.

Applicable groups for Cisco Smart PHY are `admin` and `api-admin`. By default, the `admin` user is mapped to group `admin`.

```
product opshub# smiuser assign-user-group username <username> groupname <groupname>
message User assigned to group successfully
product opshub
```

Example:

```
product opshub# smiuser assign-user-group username user123 groupname api-admin
message User assigned to group successfully
product opshub
```

Database Backup

The Database Backup section includes the following entry fields:

- Server
- Username
- Password
- Directory
- Filename (Used exclusively for the Database Import function.)

The data that you enter in the **Server** field determines the location of the DB operation.

- Local backup—localhost
- Remote operation—IP address or hostname.domain.com

Local Backup

Local backup files are saved to the `/var/smartphy/backup` directory on the local filesystem.

1. Go to **RPD Automation**> **Global Settings** > **Database Backup**.
2. In the Server field enter **localhost**.

   Leave the remaining fields blank (Username, Password, Directory, and Filename).
3. Click the **Export** button.

Remote Backup

Remote backup files are saved to the remote server at the specified file path.

1. Go to **RPD Automation**> **Global Settings** > **Database Backup**.
2. In the Server field enter the IP address or the `hostname.domain.com` of the remote server.

   Enter the user login credentials in the **Username** and **Password** fields.
3. In the **Directory** field, enter the file path on the remote server.

   Leave the **Filename (Import Only)** field blank.
4. Click the **Export** button.